

# RADIUS-externe verificatie op DNA-centrum en ISE 3.1 configureren

## Inhoud

---

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Verifiëren](#)

[Meer rollen](#)

---

## Inleiding

Dit document beschrijft hoe u RADIUS externe verificatie kunt configureren op Cisco DNA Center met behulp van een Cisco ISE-server waarop 3.1 release wordt uitgevoerd.

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco DNA Center en Cisco ISE zijn al geïntegreerd en de integratie bevindt zich op Active Status.

### Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco DNA Center 2.3.5.x release.
- Cisco ISE 3.1 release.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

## Configureren

Stap 1. Log in op de Cisco DNA Center GUI en navigeer naar Systeem > Instellingen > Verificatie- en beleidsservers.

Controleer of het RADIUS-protocol is geconfigureerd en of de ISE-status actief is voor de ISE Type-server.

Settings / External Services

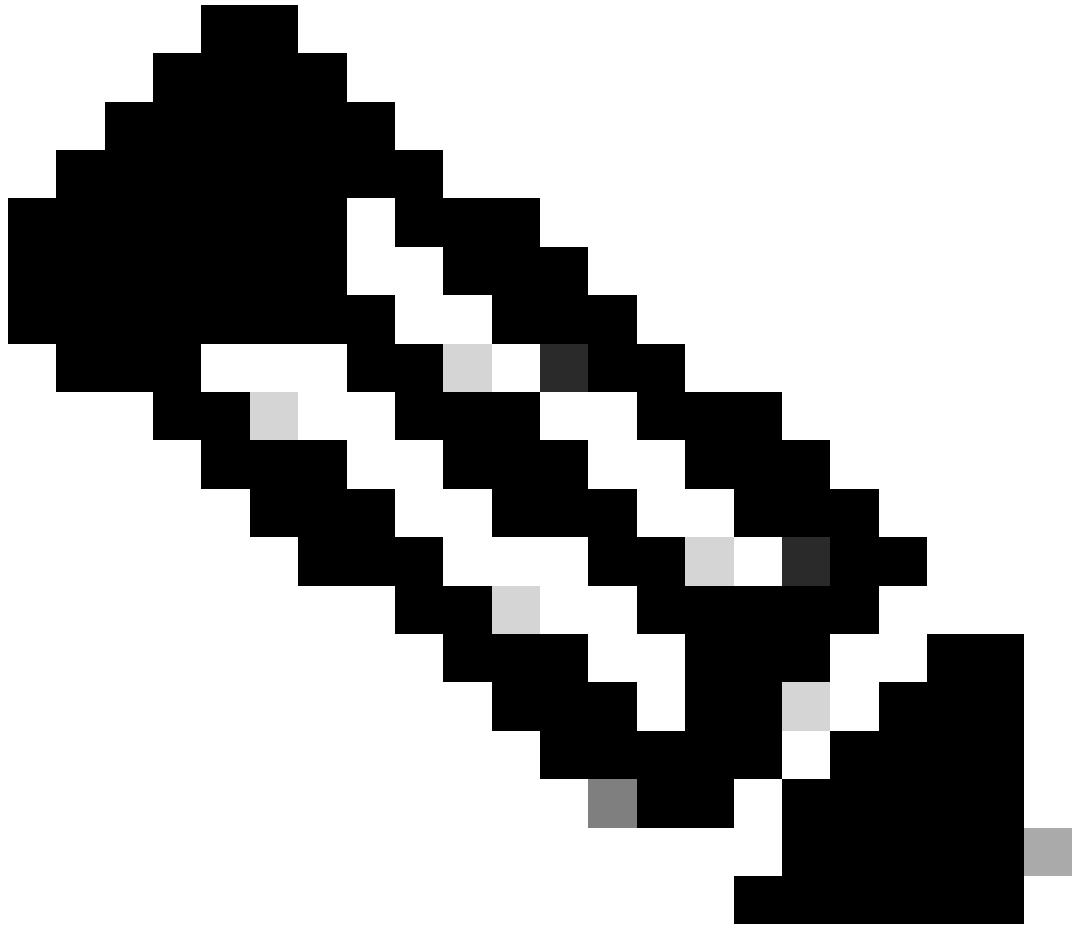
## Authentication and Policy Servers

Use this form to specify the servers that authenticate Cisco DNA Center users. Cisco Identity Services Engine (ISE) servers can also supply policy and user information.

[Add](#) [Export](#)

As of: Jul 19, 2023 4:38 PM [Refresh](#)

IP Address	Protocol	Type	Status	Actions
[REDACTED]	RADIUS_TACACS	AAA	ACTIVE	...
[REDACTED]	<b>RADIUS</b>	<b>ISE</b>	<b>ACTIVE</b>	...
[REDACTED]	RADIUS	AAA	ACTIVE	...
[REDACTED]	RADIUS	AAA	ACTIVE	...
[REDACTED]	RADIUS_TACACS	AAA	ACTIVE	...



Opmerking: het protocoltype RADIUS\_TACACS werkt voor dit document.

---














Waarschuwing: als de ISE-server niet actief is, moet u eerst de integratie oplossen.

Stap 2. Op ISE-server navigeer naar Beheer > Netwerkbronnen > Netwerkapparaten, klik op het pictogram Filter, schrijf het IP-adres van Cisco DNA Center en bevestig als een ingang bestaat. Als dit het geval is, gaat u verder naar Stap 3.

Als het bericht ontbreekt, moet u het bericht Geen gegevens beschikbaar zien.

## Network Devices

Selected 0 Total 0  

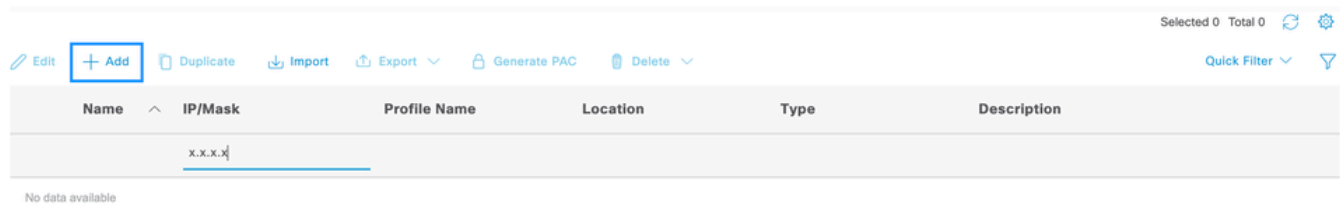
 Edit  Add  Duplicate  Import  Export  Generate PAC  Delete  Quick Filter 

Name	IP/Mask	Profile Name	Location	Type	Description
	x.x.x.x				

No data available

In dit geval moet u een netwerkapparaat maken voor Cisco DNA Center, dus klik op de knop Toevoegen.

## Network Devices



Selected 0 Total 0

Edit + Add Duplicate Import Export Generate PAC Delete Quick Filter

Name	IP/Mask	Profile Name	Location	Type	Description
	x.x.x.x				

No data available

Configureer de naam, beschrijving en IP-adres (of adressen) vanuit Cisco DNA Center. Alle andere instellingen zijn ingesteld op standaardwaarden en zijn niet nodig voor het doel van dit document.

## Network Devices

\* Name

Description

IP Address

\* Device Profile

Model Name

Software Version

\* Network Device Group

Location	<input type="text" value="All Locations"/>	<input type="button" value="Set To Default"/>
IPSEC	<input type="text" value="Is IPSEC Device"/>	<input type="button" value="Set To Default"/>
Device Type	<input type="text" value="All Device Types"/>	<input type="button" value="Set To Default"/>

Scroll naar beneden en schakel de RADIUS-verificatie-instellingen in door op het aankruisvakje te klikken en een gedeeld geheim te configureren.



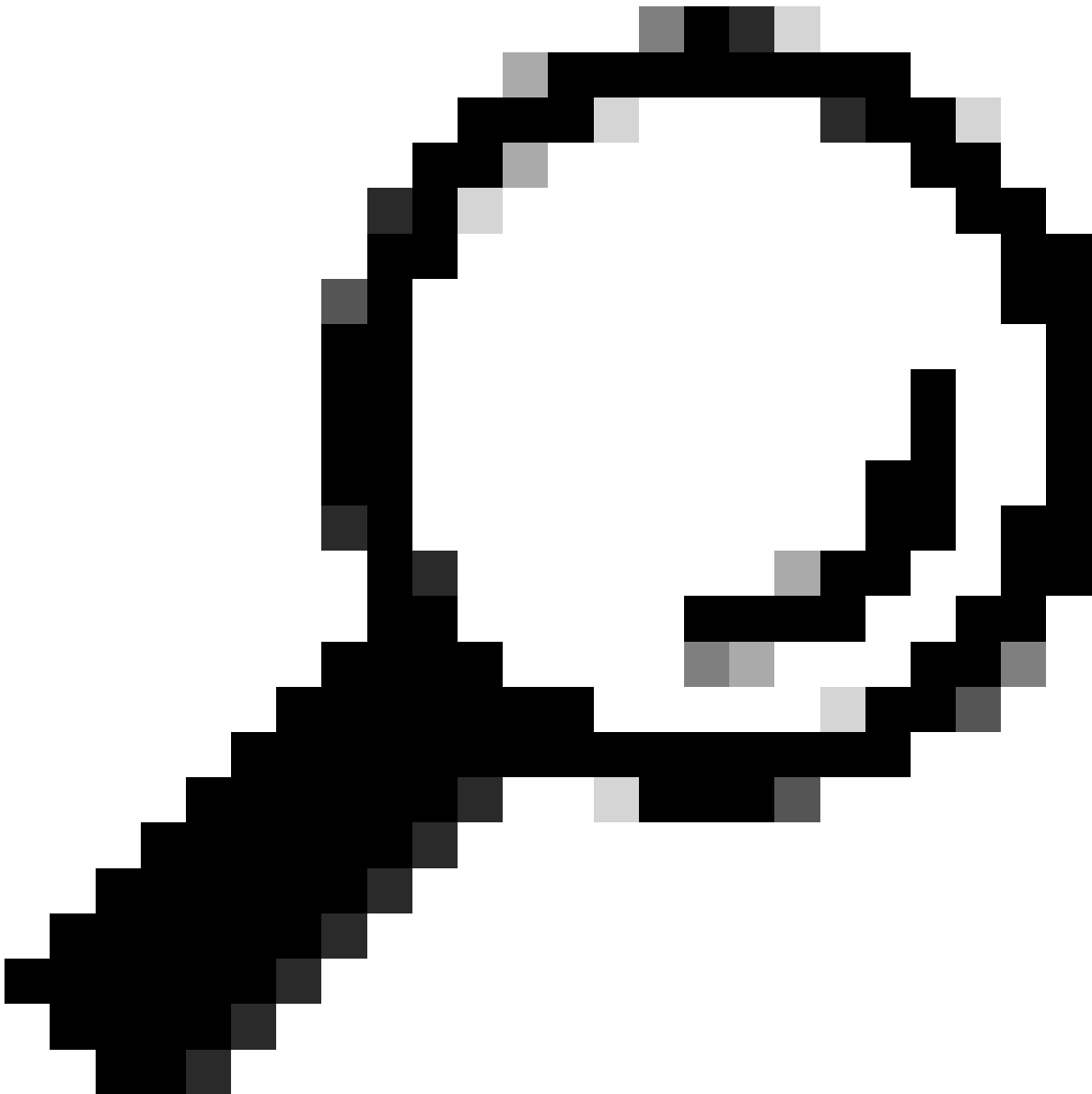
## ▼ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol **RADIUS**

\* Shared Secret .....

Show

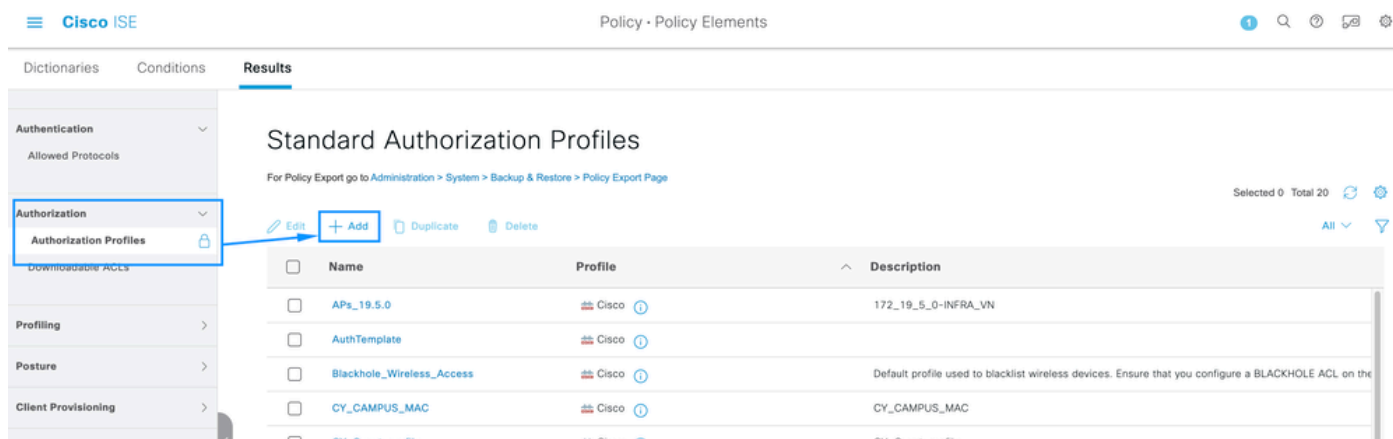


Tip: dit gedeelte geheim is later nodig, dus sla het ergens anders op.

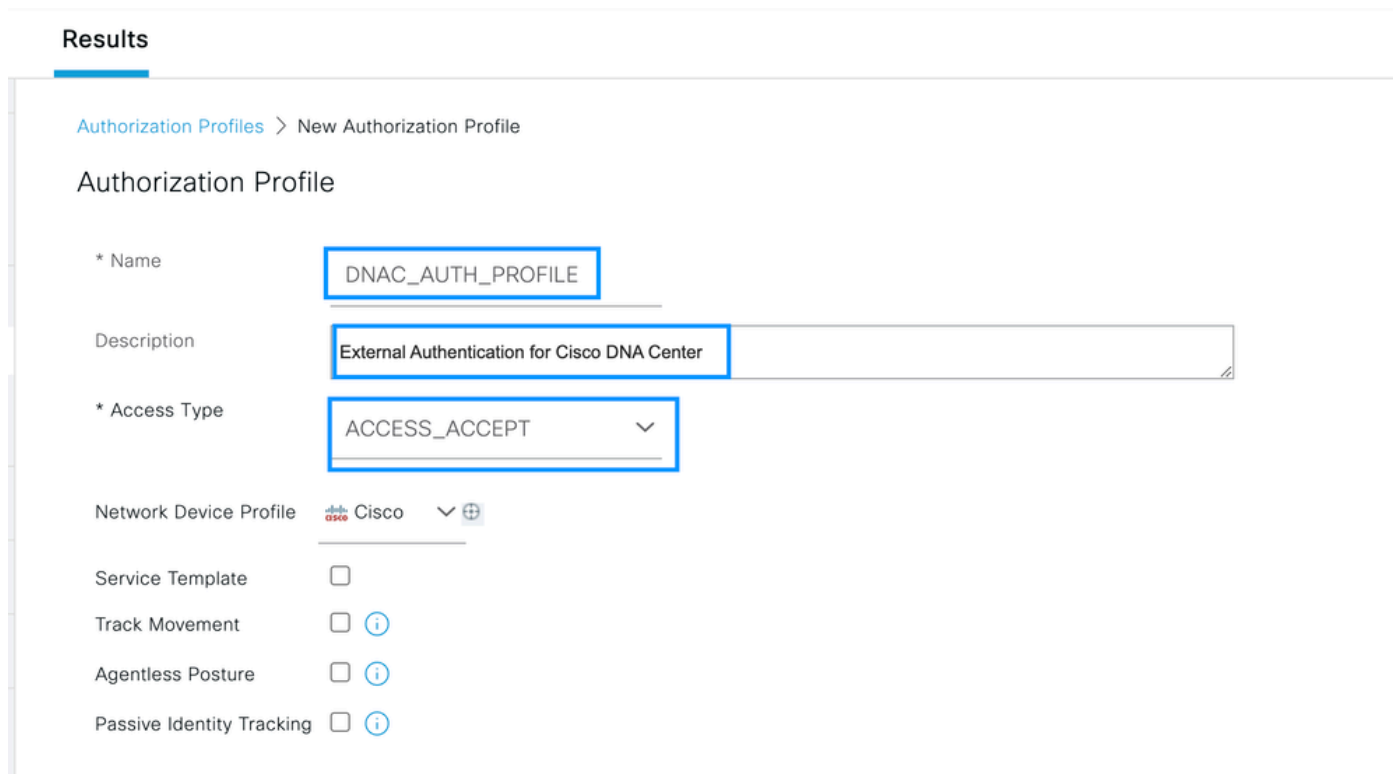
Klik vervolgens op Verzenden.

Stap 3. Op ISE Server navigeer naar Policy > Policy Elements > Results, om het autorisatieprofiel te maken.

Zorg ervoor dat u onder Autorisatie > Autorisatieprofielen staat en selecteer vervolgens de optie Toevoegen.



Naam configureren, een beschrijving toevoegen alleen om een record van het nieuwe profiel bij te houden en ervoor te zorgen dat het toegangstype is ingesteld op ACCES\_ACCEPTEREN.





Blader naar beneden en configureer de geavanceerde instellingen voor kenmerken.

Zoek in de linkerkolom naar de optie Cisco-av-pair en selecteer deze optie.

Typ in de rechterkolom handmatig het type Role=SUPER-ADMIN-ROL.

Klik op Verzenden zodra de afbeelding hieronder lijkt.

### Advanced Attributes Settings

Cisco:cisco-av-pair = Role=SUPER-ADMIN-ROLE

### Attributes Details

Access Type = ACCESS\_ACCEPT  
cisco-av-pair = Role=SUPER-ADMIN-ROLE

Stap 4. Ga op ISE-server naar Workcenters > Profiler > Policy Sets, om het verificatie- en autorisatiebeleid te configureren.

Identificeer het Standaardbeleid en klik op de blauwe pijl om het te configureren.

The screenshot shows the Cisco ISE Work Centers - Profiler interface. The 'Policy Sets' section is active, displaying a table of policy sets. The 'Default' policy set is highlighted with a blue box, and a blue arrow points to its configuration icon (a gear with a right-pointing arrow).

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
⊗	Wire-dot1x		Wired_802.1X	internal_user	0	⚙️	➔
⊗	MAB		Wired_MAB	Default Network Access	0	⚙️	➔
✅	Default	Default policy set		Default Network Access	180517	⚙️	➔

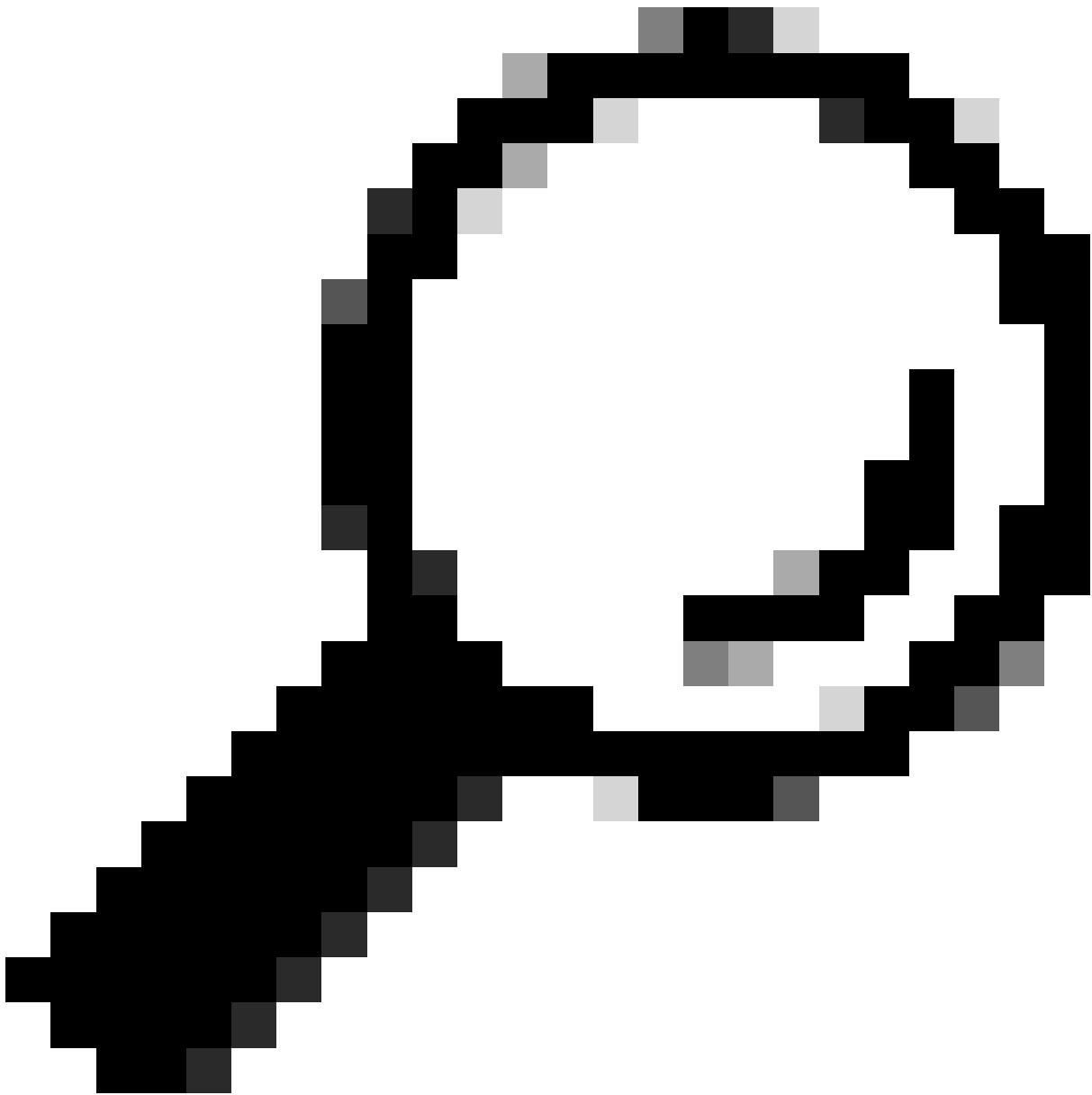
Vouw in de Default Policy Set het verificatiebeleid uit en vouw onder de sectie Default de opties uit en zorg ervoor dat deze overeenkomen met de onderstaande configuratie.

The screenshot displays the Cisco ISE Work Centers - Profiler interface. At the top, there is a navigation bar with the Cisco ISE logo and the title 'Work Centers - Profiler'. Below this is a menu with various options: Overview, Ext Id Sources, Network Devices, Endpoint Classification, Node Config, Feeds, Manual Scans, Policy Elements, Profiling Policies, and More. The main content area is titled 'Policy Sets -> Default' and includes buttons for 'Reset', 'Reset Policyset Hitcounts', and 'Save'. A table lists the policy sets, with the 'Default' policy set selected. Below this, a section titled 'Authentication Policy (3)' is expanded, showing three rules: 'MAB', 'Dot1X', and 'Default'. The 'Default' rule is selected, and its configuration is shown in a detailed view. This view includes a search bar, a table with columns for Status, Rule Name, Conditions, Use, Hits, and Actions. The 'Default' rule has a status of 'On', a rule name of 'Default', and conditions for 'Wired\_MAB' and 'Wireless\_MAB'. The 'Use' column shows 'Internal Endpoints' and 'Options'. The 'Hits' column shows '4556'. The 'Actions' column shows 'Options'. The 'Options' section is expanded, showing three conditions: 'If Auth fail', 'If User not found', and 'If Process fail'. The actions for these conditions are 'REJECT', 'REJECT', and 'DROP' respectively. Blue arrows point to these actions, and a blue box highlights the 'Options' dropdown menu.

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
On	Default	Default policy set		Default Network Access	180617

Status	Rule Name	Conditions	Use	Hits	Actions
On	MAB	OR Wired_MAB Wireless_MAB	Internal Endpoints > Options	4556	Options
On	Dot1X	OR Wired_802.1X Wireless_802.1X	All_User_ID_Stores > Options	0	Options
On	Default		All_User_ID_Stores Options If Auth fail REJECT If User not found REJECT If Process fail DROP	62816	Options



Tip: REJECT geconfigureerd op de 3 opties werkt ook

---

In de Default Policy Set vouwt u het autorisatiebeleid uit en selecteert u het pictogram Add om een nieuwe autorisatievoorwaarde te maken.

Cisco ISE Work Centers - Profiler

Overview Ext Id Sources Network Devices Endpoint Classification Node Config Feeds Manual Scans Policy Elements Profiling Policies More

Policy Sets → Default Reset Reset Policyset Hitcounts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Default	Default policy set		Default Network Access	180617

> Authentication Policy (3)

> Authorization Policy - Local Exceptions

> Authorization Policy - Global Exceptions

Authorization Policy (25)

Status	Rule Name	Conditions	Results		Hits	Actions
			Profiles	Security Groups		
+						

Configureer een regelnaam en klik op het pictogram Add om de Conditie te configureren.

Cisco ISE Work Centers - Profiler

Overview Ext Id Sources Network Devices Endpoint Classification Node Config Feeds Manual Scans Policy Elements Profiling Policies More

Policy Sets → Default Reset Reset Policyset Hitcounts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Default	Default policy set		Default Network Access	180617

> Authentication Policy (3)

> Authorization Policy - Local Exceptions

> Authorization Policy - Global Exceptions

Authorization Policy (26)

Status	Rule Name	Conditions	Results		Hits	Actions
			Profiles	Security Groups		
✓	DNAC-SUPER-ADMIN-ROLE					

Als deel van de voorwaarde, associeer het met het IP-adres van het netwerkapparaat dat in stap 2 is geconfigureerd.

# Conditions Studio

## Library

Search by Name



- BYOD\_is\_Registered
- Catalyst\_Switch\_Local\_Web\_Authentication
- Compliance\_Unknown\_Devices
- Compliant\_Devices
- CY\_Campus
- CY\_CAMPUS\_MAC
- CY\_Campus\_voice
- CY\_Guest
- EAP-MSCHAPv2

## Editor

Network Access-Device IP Address

Equals 10.88.244.151

Set to 'Is not'

Duplicate Save

NEW AND OR

Close

Use

Klik op Opslaan.

Sla het op als een nieuwe bibliotheekvoorwaarde, en noem het zoals u wilt, in deze zaak wordt het genoemd alsDNAC.



# Save condition

Save as existing Library Condition (replaces current version and impact all policies that use this condition)

Select from list ▼

Save as a new Library Condition

DNAC

Description (optional)

Condition Description

Close

Save

Configureer tot slot het profiel dat bij stap 3 is gemaakt.

The screenshot shows the Cisco ISE Work Centers - Profiler interface. The top navigation bar includes 'Cisco ISE' and 'Work Centers - Profiler'. The main content area displays a table of Policy Sets. The first row is 'Default' with a status of 'On' and a description of 'Default policy set'. Below this, there are expandable sections for 'Authentication Policy (3)', 'Authorization Policy - Local Exceptions', 'Authorization Policy - Global Exceptions', and 'Authorization Policy (25)'. The 'Authorization Policy (25)' section is expanded, showing a table with columns for 'Status', 'Rule Name', 'Conditions', 'Profiles', 'Security Groups', 'Hits', and 'Actions'. The first row in this table is 'DNAC-SUPER-ADMIN-ROLE' with a status of 'On' and conditions of 'DNAC'. The 'Profiles' column for this row shows 'DNAC\_AUTH\_PROFILE' with a dropdown arrow and a plus sign. The 'Security Groups' column shows 'Select from list' with a dropdown arrow and a plus sign.

Klik op Opslaan.

Stap 5. Log in op de Cisco DNA Center GUI en navigeer naar Systeem > Gebruikers en rollen > Externe verificatie.

Klik op de optie Externe gebruiker inschakelen en stel het AAA-kenmerk in als Cisco-AVPair.

User Management

Role Based Access Control

External Authentication

## External Authentication

Cisco DNA Center supports external servers for authentication and authorization of External Users. Use the fields in this window to create, update and on Cisco DNA Center is the name of the AAA attribute chosen on the AAA server. The default attribute expected is Cisco-AVPair, but if the user choos it needs to be configured here on Cisco DNA Center.

The value of the AAA attribute to be configured for authorization on AAA server would be in the format of "Role=role1". On ISE server, choose the cisco attributes list. A sample configuration inside Authorization profile would look like "cisco-av-pair= Role=SUPER-ADMIN-ROLE".

An example configuration in the case of manually defining the AAA attribute would be "Cisco-AVPair=Role=SUPER-ADMIN-ROLE".

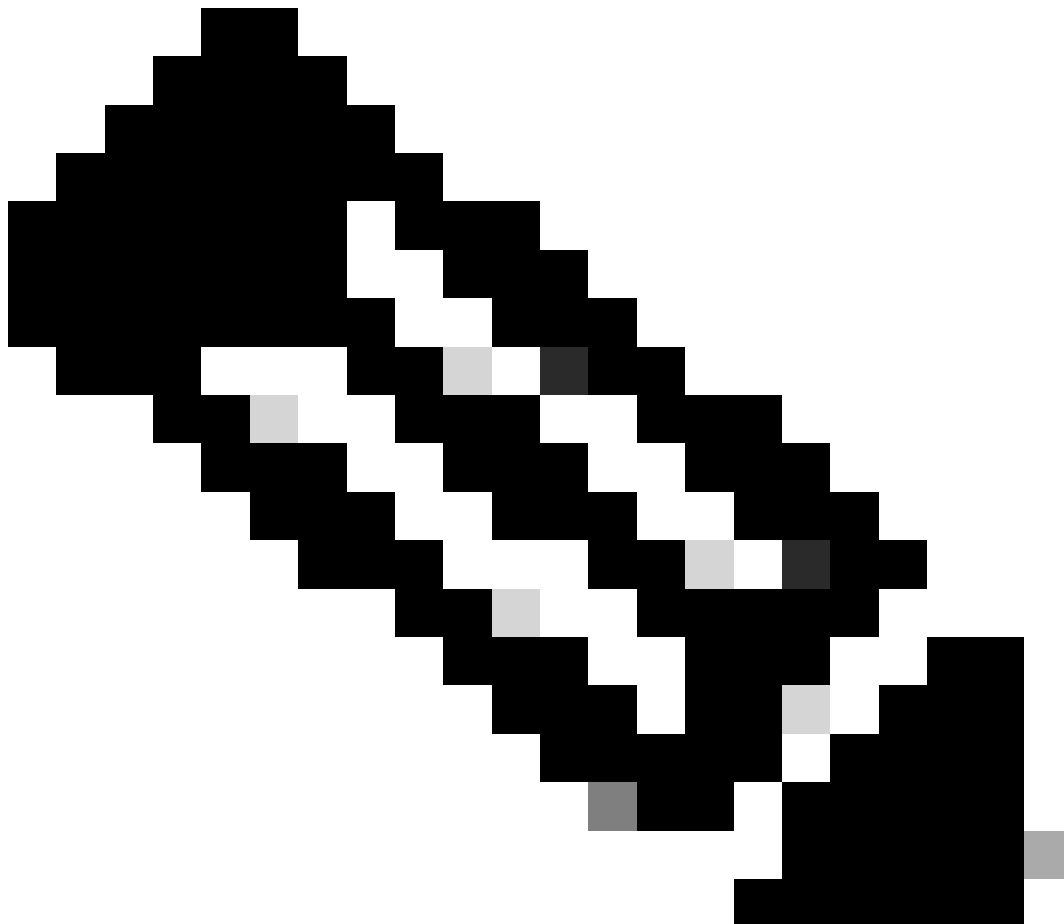
Enable External User ?

AAA Attribute

Cisco-AVPair

Reset to Default

Update



Opmerking: ISE Server gebruikt het kenmerk Cisco-AVPair op de backend, dus de

---

configuratie op Stap 3 is geldig.

---

Blader omlaag om de configuratiesectie van de AAA-server(s) te zien. Configureer het IP-adres vanaf ISE-server in stap 1 en stel het gedeelde geheim in als configuratie in stap 3.

Klik vervolgens op Geavanceerde instellingen bekijken.

✓ AAA Server(s)

### Primary AAA Server

IP Address

10.10.10.10



Shared Secret

\*\*\*\*\*

SHOW

Info

View Advanced Settings

Update

### Secondary AAA Server

IP Address

10.10.10.10



Shared Secret

\*\*\*\*\*

SHOW

Info

View Advanced Settings

Update

Controleer of de RADIUS-optie is geselecteerd en klik op de knop Bijwerken op beide servers.



✓ AAA Server(s)

### Primary AAA Server

IP Address

██████████



Shared Secret

\*\*\*\*\*

SHOW

Info

Hide Advanced Settings

RADIUS  TACACS

Authentication Port

1812

Accounting Port

1813

Retries

3

Timeout (seconds)

4

### Secondary AAA Server

IP Address

██████████



Shared Secret

\*\*\*\*\*

SHOW

Info

Hide Advanced Settings

RADIUS  TACACS

Authentication Port

1812

Accounting Port

1813

Retries

3

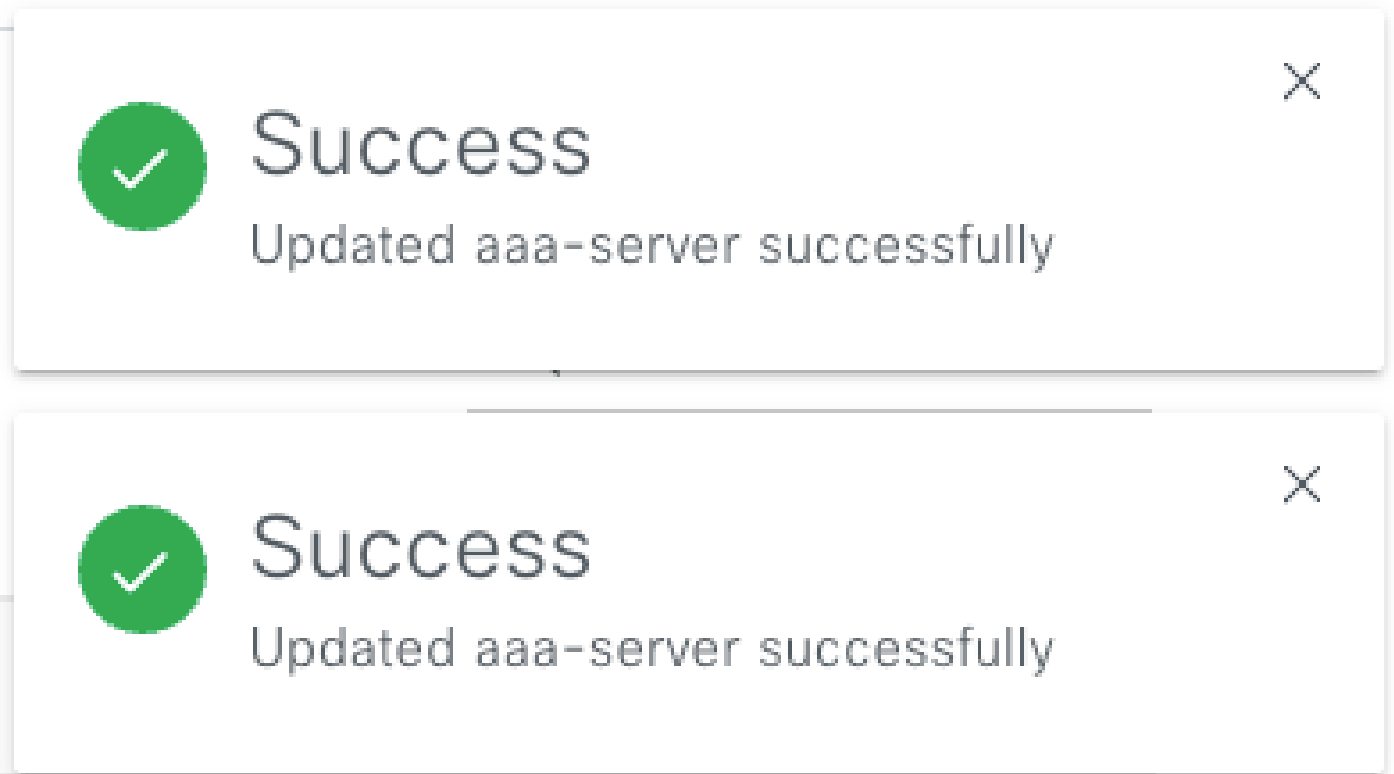
Timeout (seconds)

4

Update

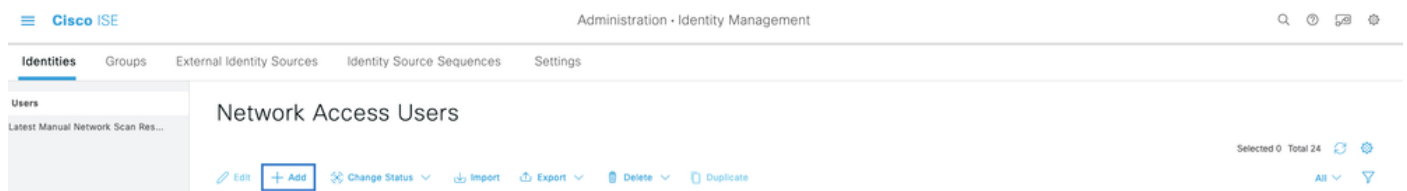
Update

U moet een Success-bericht zien voor elke sessie.



U kunt nu inloggen met een ISE-identiteit die is gemaakt in het menu ISE > Beheer > Identity Management > Identity > Identity > Gebruikers.

Mocht u nog geen aangemaakt hebben, meld u dan aan bij ISE, navigeer dan naar het bovenstaande pad en voeg een nieuwe gebruiker voor netwerktoegang toe.



## Verifiëren

De Cisco DNA Center GUI laden en Log in met een gebruiker van ISE-identiteiten.



# Cisco DNA Center

The bridge to possible

✓ Success!

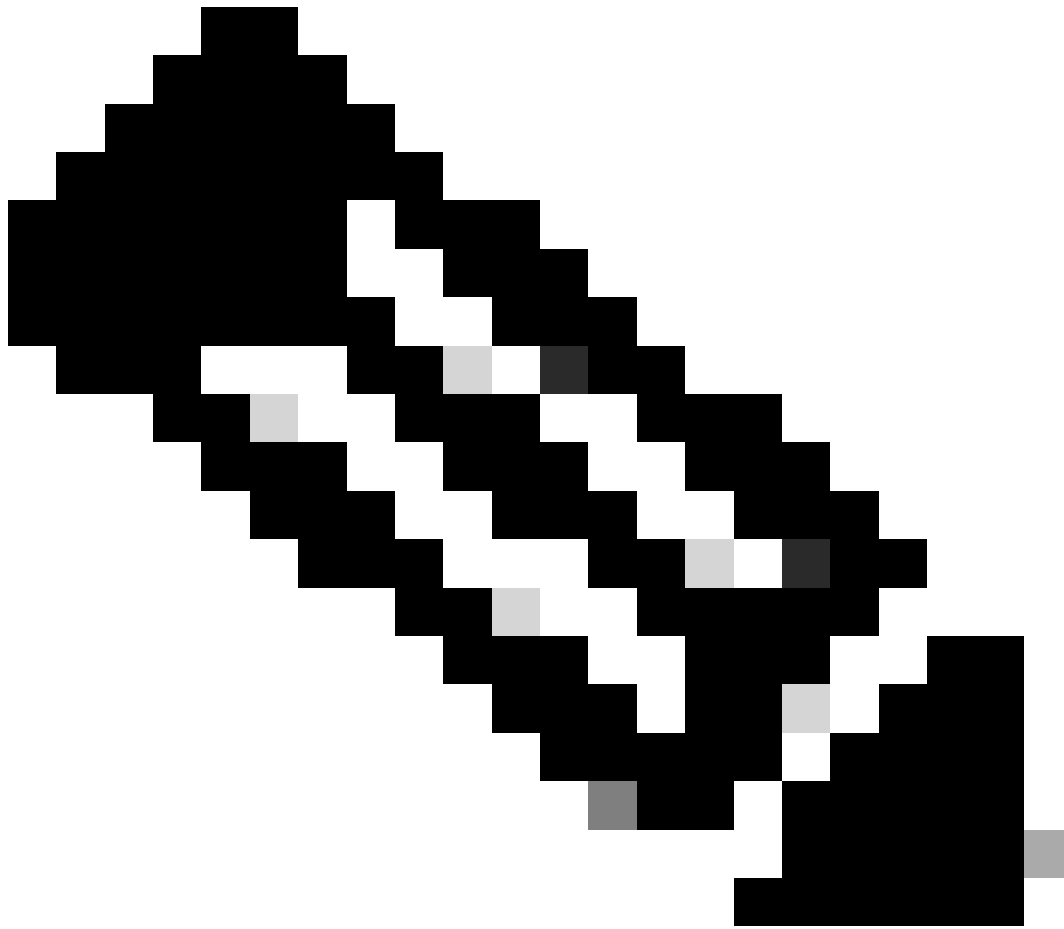
Username

test

Password

.....

Log In



Opmerking: elke gebruiker van ISE-identiteiten kan nu inloggen. U kunt meer granulariteit toevoegen aan de verificatieregels op ISE-server.

---

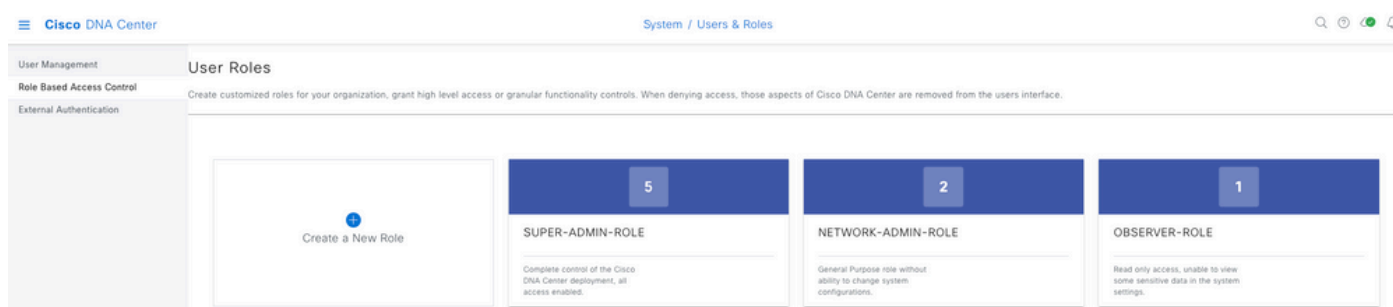
Nadat het inloggen is geslaagd, wordt de gebruikersnaam weergegeven op de Cisco DNA Center GUI

## Welcome, test

Welkomstscherm

### Meer rollen

U kunt deze stappen voor elke rol op Cisco DNA Center herhalen, standaard hebben we: SUPER-ADMIN-ROL, NETWORK-ADMIN-ROL en OBSERVER-ROL.



In dit document gebruiken we het voorbeeld SUPER-ADMIN-ROL, maar u kunt één autorisatieprofiel op ISE configureren voor elke rol in Cisco DNA Center. De enige overweging is dat de rol die op Stap 3 is geconfigureerd exact (hoofdlettergevoelig) moet overeenkomen met de Rol naam op Cisco DNA Center.

## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.